

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 determining whether a source address for a first packet sent by the source address to a
3 destination address qualifies as a threat;
4 examining the first packet; and
5 determining a response to the first packet based upon the examining.

1 2. The method of claim 1 further comprising:
2 when the source address qualifies as the threat,
3 determining whether the destination address is synthetic.

1 3. The method of claim 2 further comprising:
2 when the destination address is synthetic,
3 determining the response to be dropping the first packet.

1 4. The method of claim 3 further comprising:
2 dropping the first packet.

1 5. The method of claim 2 further comprising:
2 when the destination address is not synthetic,
3 determining whether the source address is on a local network.

1 6. The method of claim 5 further comprising:
2 when the source address is not on the local network,
3 determining that the response is to perform for each respective device of a plurality of
4 devices on the local network:
5 selecting the respective device,
6 creating a respective synthetic hardware address for the respective device,
7 creating an address control protocol message comprising
8 the respective synthetic hardware address as a message source address,
9 inserting a corresponding hardware address for a gateway communicating on
10 behalf of the source address in the address control protocol message as
11 a message destination hardware address, and
12 sending the address control protocol message.

1 7. The method of claim 6 further comprising:
2 performing the response.

1 8. The method of claim 6 wherein
2 the creating the respective synthetic hardware address for the respective device comprises
3 ensuring that the respective synthetic hardware address is not in use on the local
4 network.

1 9. The method of claim 6 further comprising:
2 inserting a corresponding logical address for the gateway in the address control protocol
3 message as a message destination logical address.

1 10. The method of claim 6 wherein
2 the gateway inserts an entry into an address resolution protocol table in response to receiving
3 the address resolution protocol message, wherein
4 the entry comprises
5 the respective synthetic hardware address for the respective device.

1 11. The method of claim 5 further comprising:
2 when the source address is on a local network, determining that the response comprises
3 creating a synthetic hardware address, and
4 performing for each respective device of a plurality of devices on the local network:
5 selecting the respective device,
6 creating an address control protocol message comprising
7 the synthetic hardware address as a message source address,
8 inserting a corresponding hardware address for the respective device in the
9 address control protocol message as a message destination hardware
10 address, and
11 sending the address control protocol message.

1 12. The method of claim 11 further comprising:
2 performing the response.

1 13. The method of claim 11 wherein
2 the creating the synthetic hardware address comprises ensuring that the synthetic hardware
3 address is not in use on the local network.

1 14. The method of claim 11 further comprising:
2 inserting a corresponding logical address for the respective device in the address control
3 protocol message as a message destination logical address.

1 15. The method of claim 11 wherein
2 the respective device inserts an entry into an address resolution protocol table in response to
3 receiving the address resolution protocol message, wherein
4 the entry comprises
5 the synthetic hardware address as a source hardware address for the source
6 address.

1 16. The method of claim 5 further comprising:
2 when the source address is on the local network,
3 determining that the response is to perform for each respective device of a plurality of
4 devices on the local network:
5 selecting the respective device,
6 creating a respective synthetic hardware address for the respective device,
7 creating an address control protocol message comprising
8 the respective synthetic hardware address as a message source address,
9 inserting the source address in the address control protocol message as a
10 message destination hardware address, and
11 sending the address control protocol message.

1 17. The method of claim 16 further comprising:
2 performing the response.

1 18. The method of claim 16 wherein
2 the creating the respective synthetic hardware address for the respective device comprises
3 ensuring that the respective synthetic hardware address is not in use on the local
4 network.

1 19. The method of claim 16 further comprising:
2 inserting a corresponding logical address for the source address in the address control
3 protocol message as a message destination logical address.

1 20. The method of claim 16 wherein
2 the source address inserts an entry into an address resolution protocol table in response to
3 receiving the address resolution protocol message, wherein
4 the entry comprises
5 the respective synthetic hardware address for the respective device.

1 21. The method of claim 1 further comprising:
2 when the source address fails to qualify as the threat,
3 determining whether the destination address qualifies as a second threat.

1 22. The method of claim 21 further comprising:
2 when the destination address qualifies as the second threat,
3 determining whether the destination address comprises a synthetic hardware address,
4 and
5 when the destination address is a synthetic hardware address,
6 determining the response to be dropping the first packet.

1 23. The method of claim 22 further comprising:
2 dropping the first packet.

1 24. The method of claim 21 further comprising:
2 when the destination address fails to qualify as the second threat,
3 determining whether the destination address is a synthetic hardware address,
4 and
5 when the destination address is the synthetic hardware address, determining the
6 response to comprise
7 modifying the first packet by replacing the destination address with a
8 hardware address for a device at the destination address; and
9 sending the first packet.

1 25. The method of claim 24 further comprising:
2 performing the response.

1 26. The method of claim 1 further comprising:
2 when the source address qualifies as the threat,
3 determining a packet type of the first packet.

1 27. The method of claim 26 further comprising:
2 when the packet type of the first packet is an address resolution protocol request,
3 determining that the response comprises
4 creating a reply comprising the destination address as a reply source address,
5 and
6 sending the reply to the source address.

1 28. The method of claim 26 further comprising:
2 when the packet type of the first packet is an internet common message protocol echo
3 request,
4 determining that the response comprises
5 creating a reply to indicate that the destination address is active; and
6 sending the reply to the source address.

1 29. The method of claim 26 further comprising:
2 when the packet type of the first packet is transmission control protocol,
3 determining whether the first packet is a transmission control protocol syn request;
4 when the first packet is the transmission control protocol syn request,
5 determining that the response comprises
6 creating a transmission control protocol syn response indicating
7 that the source address must receive an
8 acknowledgement for each subsequent packet before the
9 source address can transmit another subsequent packet;
10 and
11 sending the transmission control protocol syn response to the
12 source address.

1 30. The method of claim 26 further comprising:
2 when the packet type of the first packet is transmission control protocol,
3 determining whether the first packet is a transmission control protocol syn request;
4 when the first packet is the transmission control protocol syn request,
5 determining that the response comprises
6 creating a transmission control protocol syn response
7 comprising a payload; and
8 sending the transmission control protocol syn response to the
9 source address.

1 31. The method of claim 30 wherein
2 a size of the payload is smaller than a maximum size permitted by a network by which the
3 first packet was transmitted.

1 32. The method of claim 26 further comprising:
2 when the packet type of the first packet is transmission control protocol,
3 determining whether the first packet is a transmission control protocol window probe;
4 and
5 when the first packet is the transmission control protocol window probe,
6 determining that the response comprises
7 creating a transmission control protocol window probe
8 response comprising a transmission control protocol
9 window size of zero, and
10 sending the transmission control protocol window probe
11 response to the source address.

1 33. The method of claim 26 further comprising:
2 when the packet type of the first packet is transmission control protocol,
3 determining whether the first packet is a transmission control protocol window probe;
4 when the first packet is the transmission control protocol window probe,
5 determining that the response comprises
6 creating a transmission control protocol syn response
7 comprising a payload; and

8 sending the transmission control protocol syn response to the
9 source address.

1 34. The method of claim 33 wherein
2 a size of the payload is smaller than a maximum size permitted by a network by which the
3 first packet was transmitted.

1 35. The method of claim 26 further comprising:
2 when the packet type of the first packet is transmission control protocol,
3 determining whether the first packet is a transmission control protocol
4 acknowledgement;
5 and
6 when the first packet is the transmission control protocol acknowledgement,
7 determining that the response comprises
8 ignoring the first packet.

1 36. The method of claim 26 further comprising:
2 performing the response.

1 37. The method of claim 1 wherein
2 the source address comprises at least one of a logical address and a physical address.

1 38. The method of claim 1 wherein
2 the destination address comprises a logical address.

1 39. The method of claim 1 wherein
2 the examining the first packet comprises examining a header for the first packet.

1 40. The method of claim 1 wherein
2 the examining the first packet does not comprise examining a payload for the first packet.

1 41. A method comprising: ✓
2 examining a first packet sent by a source address to a destination address;
3 determining whether the destination address is a synthetic hardware address; and
4 when the destination address is the synthetic hardware address,

5 modifying the first packet by replacing the destination address with a
6 hardware address for a device to receive communication targeted to the
7 destination address, and
8 sending the first packet.

1 42. A system comprising:
2 threat-determining means for determining whether a source address for a first packet sent by
3 the source address to a destination address qualifies as a threat;
4 examining means for examining the first packet; and
5 response-determining means for determining a response to the first packet based upon the
6 examining.

1 43. The system of claim 42 further comprising:
2 synthetic-address-determining means for determining whether the destination address is
3 synthetic.

1 44. The system of claim 43 wherein:
2 the response-determining means determine the response to be dropping the first packet when
3 the destination address is synthetic.

1 45. The system of claim 44 further comprising:
2 dropping means for dropping the first packet.

1 46. The system of claim 42 further comprising:
2 location-determining means for determining whether the source address is on a local network.

1 47. The system of claim 46 wherein
2 when the location-determining means determine that the source address is not on the local
3 network,

4 the response-determining means are configured to determine that the response is to
5 perform for each respective device of a plurality of devices on the local
6 network:

7 select the respective device,

8 create a respective synthetic hardware address for the respective device,

9 create an address control protocol message comprising

10 the respective synthetic hardware address as a message source address,

11 insert a corresponding hardware address for a gateway communicating on
 12 behalf of the source address in the address control protocol message as
 13 a message destination hardware address, and
 14 send the address control protocol message.

1 48. The system of claim 46 wherein
 2 when the location-determining means determine that the source address is on the local
 3 network,
 4 the response-determining means are configured to determine that the response is to
 5 create a synthetic hardware address, and
 6 perform for each respective device of a plurality of devices on the local
 7 network:
 8 select the respective device,
 9 create an address control protocol message comprising
 10 the synthetic hardware address as a message source address,
 11 insert a corresponding hardware address for the respective device in
 12 the address control protocol message as a message destination
 13 hardware address, and
 14 send the address control protocol message.

1 49. The system of claim 46 wherein
 2 when the location-determining means determine that the source address is on the local
 3 network,
 4 the response-determining means are configured to determine that the response is to
 5 perform for each respective device of a plurality of devices on the local
 6 network:
 7 select the respective device,
 8 create a respective synthetic hardware address for the respective device,
 9 create an address control protocol message comprising
 10 the respective synthetic hardware address as a message source address,
 11 insert the source address in the address control protocol message as a message
 12 destination hardware address, and
 13 send the address control protocol message.

1 50. The system of claim 42 further comprising:
2 second threat-determining means for determining whether the destination address qualifies as
3 a second threat.

1 51. The system of claim 50 further comprising:
2 second synthetic-address-determining means for determining whether the destination address
3 is a synthetic hardware address.

1 52. The system of claim 51, wherein
2 when the second synthetic-address-determining means determine that the destination address
3 is the synthetic hardware address,
4 the response-determining means are configured to determine that the response
5 comprises
6 modifying the first packet by replacing the destination address with a
7 hardware address for a device at the destination address, and
8 sending the first packet.

1 53. The system of claim 42 further comprising:
2 packet-type-determining means for determining a packet type of the first packet.

1 54. The system of claim 53 wherein
2 when the packet-type-determining means determine that the packet type of the first packet is
3 an address resolution protocol request,
4 the response-determining means are configured to determine that the response
5 comprises
6 creating a reply comprising the destination address as a reply source address,
7 and
8 sending the reply to the source address.

1 55. The system of claim 42 further comprising:
2 performing means for performing the response.

1 56. A system comprising: ↘
2 examining means for examining a first packet sent by a source address to a destination
3 address;

4 determining means for determining whether the destination address is a synthetic hardware
5 address;
6 modifying means for modifying the first packet by replacing the destination address with a
7 hardware address for a device to receive communication targeted to the destination
8 address when the destination address is the synthetic hardware address; and
9 sending means for sending the first packet when the destination address is the synthetic
10 hardware address.

1 57. A system comprising:
2 a threat-determining module configured to determine whether a source address for a first
3 packet sent by the source address to a destination address qualifies as a threat;
4 an examining module configured to examine the first packet; and
5 a response-determining module configured to determine a response to the first packet based
6 upon the examining.

1 58. The system of claim 57 further comprising:
2 a synthetic-address-determining module configured to determine whether the destination
3 address is synthetic.

1 59. The system of claim 58 wherein:
2 the response-determining module determines the response to be dropping the first packet
3 when the destination address is synthetic.

1 60. The system of claim 59 further comprising:
2 a dropping module configured to drop the first packet.

1 61. The system of claim 57 further comprising:
2 a location-determining module configured to determine whether the source address is on a
3 local network.

1 62. The system of claim 61 wherein
2 when the location-determining module determines that the source address is not on the local
3 network,
4 the response-determining module is configured to determine that the response is to
5 perform for each respective device of a plurality of devices on the local
6 network:

7 select the respective device,
8 create a respective synthetic hardware address for the respective device,
9 create an address control protocol message comprising
10 the respective synthetic hardware address as a message source address,
11 insert a corresponding hardware address for a gateway communicating on
12 behalf of the source address in the address control protocol message as
13 a message destination hardware address, and
14 send the address control protocol message.

1 63. The system of claim 61 wherein
2 when the location-determining module determines that the source address is on the local
3 network,
4 the response-determining means are configured to determine that the response is to
5 create a synthetic hardware address, and
6 perform for each respective device of a plurality of devices on the local
7 network:
8 select the respective device,
9 create an address control protocol message comprising
10 the synthetic hardware address as a message source address,
11 insert a corresponding hardware address for the respective device in
12 the address control protocol message as a message destination
13 hardware address, and
14 send the address control protocol message.

1 64. The system of claim 61 wherein
2 when the location-determining module determines that the source address is on the local
3 network,
4 the response-determining module is configured to determine that the response is to
5 perform for each respective device of a plurality of devices on the local
6 network:
7 select the respective device,
8 create a respective synthetic hardware address for the respective device,
9 create an address control protocol message comprising
10 the respective synthetic hardware address as a message source address,

11 insert the source address in the address control protocol message as a message
12 destination hardware address, and
13 send the address control protocol message.

1 65. The system of claim 57 further comprising:
2 a second threat-determining module configured to determine whether the destination address
3 qualifies as a second threat.

1 66. The system of claim 57 further comprising:
2 a second synthetic-address-determining module configured to determine whether the
3 destination address is a synthetic hardware address.

1 67. The system of claim 66, wherein
2 when the second synthetic-address-determining module determines that the destination
3 address is the synthetic hardware address,
4 the response-determining module is configured to determine that the response
5 comprises
6 modifying the first packet by replacing the destination address with a
7 hardware address for a device at the destination address, and
8 sending the first packet.

1 68. The system of claim 57 further comprising:
2 a packet-type-determining module configured to determine a packet type of the first packet.

1 69. The system of claim 68 wherein
2 when the packet-type-determining module determines that the packet type of the first packet
3 is an address resolution protocol request,
4 the response-determining module is configured to determine that the response
5 comprises
6 creating a reply comprising the destination address as a reply source address,
7 and
8 sending the reply to the source address.

1 70. The system of claim 57 further comprising:
2 a performing module configured to perform the response.

1 71. A system comprising: ↵
2 an examining module configured to examine a first packet sent by a source address to a
3 destination address;
4 a determining module configured to determine whether the destination address is a synthetic
5 hardware address;
6 a modifying module configured to modify the first packet by replacing the destination
7 address with a hardware address for a device to receive communication targeted to the
8 destination address when the destination address is the synthetic hardware address;
9 and
10 a sending module configured to send the first packet when the destination address is the
11 synthetic hardware address.

1 72. A computer-readable medium comprising: ↵
2 threat-determining instructions configured to determine whether a source address for a first
3 packet sent by the source address to a destination address qualifies as a threat;
4 examining instructions configured to examine the first packet; and
5 response-determining instructions configured to determine a response to the first packet
6 based upon the examining.

1 73. The computer-readable medium of claim 72 further comprising:
2 synthetic-address-determining instructions configured to determine whether the destination
3 address is synthetic.

1 74. The computer-readable medium of claim 73 wherein:
2 the response-determining instructions determines the response to be dropping the first packet
3 when the destination address is synthetic.

1 75. The computer-readable medium of claim 74 further comprising:
2 dropping instructions configured to drop the first packet.

1 76. The computer-readable medium of claim 72 further comprising:
2 location-determining instructions configured to determine whether the source address is on a
3 local network.

1 77. The computer-readable medium of claim 76 wherein
2 when the location-determining instructions determines that the source address is not on the
3 local network,
4 the response-determining instructions is configured to determine that the response is
5 to perform for each respective device of a plurality of devices on the local
6 network:
7 select the respective device,
8 create a respective synthetic hardware address for the respective device,
9 create an address control protocol message comprising
10 the respective synthetic hardware address as a message source address,
11 insert a corresponding hardware address for a gateway communicating on
12 behalf of the source address in the address control protocol message as
13 a message destination hardware address, and
14 send the address control protocol message.

1 78. The computer-readable medium of claim 76 wherein
2 when the location-determining instructions determines that the source address is on the local
3 network,
4 the response-determining means are configured to determine that the response is to
5 create a synthetic hardware address, and
6 perform for each respective device of a plurality of devices on the local
7 network:
8 select the respective device,
9 create an address control protocol message comprising
10 the synthetic hardware address as a message source address,
11 insert a corresponding hardware address for the respective device in
12 the address control protocol message as a message destination
13 hardware address, and
14 send the address control protocol message.

1 79. The computer-readable medium of claim 76 wherein
2 when the location-determining instructions determines that the source address is on the local
3 network,

the response-determining instructions is configured to determine that the response is to perform for each respective device of a plurality of devices on the local network:
select the respective device,
create a respective synthetic hardware address for the respective device,
create an address control protocol message comprising
the respective synthetic hardware address as a message source address,
insert the source address in the address control protocol message as a message destination hardware address, and
send the address control protocol message.

80. The computer-readable medium of claim 72 further comprising:
second threat-determining instructions configured to determine whether the destination address qualifies as a second threat.

81. The computer-readable medium of claim 72 further comprising:
second synthetic-address-determining instructions configured to determine whether the destination address is a synthetic hardware address.

82. The computer-readable medium of claim 81, wherein
when the second synthetic-address-determining instructions determine that the destination address is the synthetic hardware address,
the response-determining instructions is configured to determine that the response comprises
modifying the first packet by replacing the destination address with a hardware address for a device at the destination address, and
sending the first packet.

83. The computer-readable medium of claim 72 further comprising:
packet-type-determining instructions configured to determine a packet type of the first packet.

84. The computer-readable medium of claim 83 wherein
when the packet-type-determining instructions determines that the packet type of the first packet is an address resolution protocol request,

4 the response-determining instructions is configured to determine that the response
5 comprises
6 creating a reply comprising the destination address as a reply source address,
7 and
8 sending the reply to the source address.

1 85. The computer-readable medium of claim 72 further comprising:
2 performing instructions configured to perform the response.

1 86. A computer-readable medium comprising:
2 examining instructions configured to examine a first packet sent by a source address to a
3 destination address;
4 determining instructions configured to determine whether the destination address is a
5 synthetic hardware address;
6 modifying instructions configured to modify the first packet by replacing the destination
7 address with a hardware address for a device to receive communication targeted to the
8 destination address when the destination address is the synthetic hardware address;
9 and
10 sending instructions configured to send the first packet when the destination address is the
11 synthetic hardware address.